

## UNITED STATES DISTRICT COURT

for the  
Middle District of North Carolina

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

THE RESIDENCE, OUTBUILDINGS, AND  
APPURTENANCES LOCATED AT 422 FOSTER LANE,  
PITTSBORO, NC 27312

Case No. 1:24MJ <sup>24</sup>231 -1

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the \_\_\_\_\_ Middle \_\_\_\_\_ District of \_\_\_\_\_ North Carolina \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2314	Interstate transportation of stolen property
18 U.S.C. § 1341, 1343, 1349	Mail fraud, wire fraud, and conspiracy to commit mail and wire fraud
18 U.S.C. § 1956	Money laundering

The application is based on these facts:

See the attached affidavit of U.S. Postal Inspector Alberto Sanabria

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Alberto Sanabria

Applicant's signature

Alberto Sanabria, United States Postal Inspector

Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 6/5/2024

  
Judge's signature

City and state: Winston-Salem, North Carolina

Joi Elizabeth Peake, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF:

**THE RESIDENCE, OUTBUILDINGS, AND  
APPURTENANCES LOCATED AT 422 FOSTER  
LANE, PITTSBORO, NC 27312**

Case No. 1:24mj231

**AFFIDAVIT IN SUPPORT OF  
APPLICATION FOR SEARCH AND SEIZURE WARRANT**

I, Alberto G. Sanabria, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a United States Postal Inspector with the United States Postal Inspection Service (“USPIS”) and have been so employed since 2013. During this time, I have been assigned to the Financial Crimes team and Prohibited Mailing Narcotics team where my duties include the investigation of fraud-related criminal schemes and prohibited mailing of controlled substances. I have received formal classroom training from the United States Postal Service Inspection Service during the 12-week Postal Inspector Basic Training Academy in Potomac, Maryland. I have received formal instruction from U.S. Postal Inspectors as well as other federal, state, and local law enforcement agents who have done extensive work in the areas of mail fraud, wire fraud, and the use of the U.S. mail to execute fraudulent acts. Based on my training and experience, I am familiar with the current method of operation that individuals and groups use to engage in illegally obtaining merchandise from retail establishments, through theft and/or fraud, and using the U.S. mail to send and receive the merchandise.

**PURPOSE OF THE AFFIDAVIT**

2. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that Robert “Bob” Oliver (“OLIVER”) committed violations of 18



U.S.C. § 2314 (interstate transportation of stolen property), 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1349 (conspiracy to commit mail and wire fraud), and 18 U.S.C. § 1956 (money laundering) (collectively, the “SUBJECT OFFENSES”). This affidavit is made in support of an application for a warrant to search the location specifically described in Attachment A, the premises, including all outbuildings, located at 422 Foster Lane, Pittsboro, NC 27312 (the “SUBJECT PREMISES”). There is probable cause to believe that evidence of violations of the SUBJECT OFFENSES which are more specifically described in Attachment B of this Affidavit, will be found on the **SUBJECT PREMISES**. The facts and information in this affidavit are based upon my personal knowledge as well as the observations of other law enforcement agents and others involved in the investigation.

3. The **SUBJECT PREMISES** described in Attachment A, is located in Chatham County, in the Middle District of North Carolina. The **SUBJECT PERSON** described in is the owner of the **SUBJECT PREMISES** and a resident of Chatham County.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

#### **SUBJECT OFFENSES**

5. Title 18, United States Code, Section 1341 (Mail Fraud) prohibits a person having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, for the purpose of executing such scheme or artifice or attempting to do so, from placing in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or depositing or causing to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or taking or receiving therefrom, any

such matter or thing, or knowingly causing to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing.

6. Title 18, United States Code, Section 1349 (Conspiracy to Commit Mail Fraud) prohibits a person from attempting or conspiring to commit mail fraud, the commission of which was the object of the attempt or conspiracy.

7. Title 18, United States Code, Section 2314 (interstate transportation of stolen property) prohibits a person from transporting, transmitting, or transferring in interstate or foreign commerce any goods, wares, merchandise, securities, or money, of the value of \$5,000 or more, knowing the same to have been stolen, converted, or taken by fraud.

8. Title 18, United States Code, Section 1343 (wire fraud) prohibits a person from, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purposes of executing such a scheme or artifice.

9. Title 18, United States Code, Section 1956(a)(1) (money laundering) generally prohibits a person, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, from conducting or attempting to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity (A)(i) with the intent to promote the carrying on of specified unlawful activity, or (ii) with the intent to engage in conduct constituting a violation of section 7201 or 7206 of the Internal Revenue Code of 1986; or (B) knowing that the transaction is designed in whole or in part (i) to conceal or disguise the

nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity, or (ii) to avoid a transaction reporting requirement under State or Federal law.

### **DEFINITIONS**

10. The following definitions apply to this Affidavit and Attachment B:
- a. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).
  - b. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).
  - c. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software,



documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- d. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- e. “Computer software,” as used herein, is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- f. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.
- g. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

- h. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.
- i. “Short Message Service” (“SMS”), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone.
- j. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, thumb drives, SD/Micro SD cards, and other magnetic or optical media.

#### **PROBABLE CAUSE**

11. In the course of my duties as a United States Postal Inspector with the USPIS, I, alongside other law enforcement investigators and retail investigators, have been conducting a criminal investigation associated with an organized retail crime scheme involving the theft of various retail products, including over-the-counter (“OTC”) products and medications, from retail stores, pharmacies, and national supermarket chains. The products include OTC nonprescription drugs and medical devices that are approved by the Food and Drug Administration (“FDA”), non-FDA approved products such as vitamins, minerals, dietary, and health supplements, personal care products, pet medications, and other retail merchandise. This investigation has revealed a large-scale operation involving individuals, also known as “boosters,” who steal the retail products throughout the United States. These boosters then sell the items to individuals, also

known as “fences,” who are responsible for receiving the items, and selling them to end consumers through eBay.

12. Investigators identified several boosters in Indiana who are suspected of selling the items to Tina Creech Herwehe, her son Anthony McKinney, and others, at a residence located in Indianapolis, IN. Herwehe then ships the products to the **SUBJECT PERSON**, using the U.S. Mail and other carriers to the **SUBJECT PREMISES**. Investigators additionally identified other individuals in Maryland who shipped large quantities of retail products to **SUBJECT PERSON** at the **SUBJECT PREMISES**. The **SUBJECT PERSON**, who has numerous eBay accounts, then sells the products to end consumers on eBay and ships the products through the U.S. Mail. Based on eBay records associated with the **SUBJECT PERSON**’s various eBay accounts, retail investigators have estimated several million dollars in losses to retail companies as a result of the scheme.

**A. USPS Parcel 35US & USPS Parcel 14US**

13. Beginning on or about May 21, 2019, the United States Postal Inspection Service intercepted two United States Postal Service (“USPS”) parcels bearing tracking numbers EE179287535US (“Parcel 35US”) and EE391166014US (“Parcel 14US”), going to the **SUBJECT PREMISES**. Postal inspectors applied for Federal Search Warrants, and the Honorable United States Magistrate Judge Joi Elizabeth Peake signed the warrants (1:19MJ174 & 1:19MJ175). The parcels were deemed suspicious in nature because, although both were mailed from St. Louis, Missouri, one had a return address of Broadview, Illinois 60155 (1:19MJ174), and the other had a return address of Darien, Wisconsin 53114 (1:19MJ175). Both parcels had handwritten labels and were heavily taped, including all seams of the boxes.



14. The parcels were opened by postal inspectors on May 23, 2019, pursuant to the signed Federal Search Warrants. The parcels contained retail products, such as name brand OTC medication and some store-branded OTC medication, from retail stores. The two parcels contained items such as Prevagen, Viviscal, Extenz, Florastor, PlanB, Imedeen, RepHresh, PRO-B, and Zyrtec. The items were repackaged and subsequently delivered to the **SUBJECT PERSON**.

**B. eBay Accounts**

15. The investigation confirmed that the **SUBJECT PERSON** sells retail products, in part, through various eBay accounts and utilizes the **SUBJECT PREMISES** to receive, store, and ship the items. The **SUBJECT PERSON** sells the merchandise through eBay, which includes but is not limited to, Prevagen, Viviscal, Extenz, Florastor, PlanB, Imedeen, RepHresh, PRO-B, Zyrtec, and many other products. The following is a list of eBay company, also known as “eBay Store”, accounts (the “**SUBJECT BUSINESSES**”) registered to the **SUBJECT PERSON**, that, as of the day of the application for this warrant, have retail products listed for sale:

- a. carolina\_otc (seller ID name is listed as Carolina\_OTC)
- b. emily-tastic (seller ID name is listed as emilys\_finds247)
- c. olivertwistnc (seller ID name is listed as OLIVERTWIST’S SUPPLEMENTS AND MORE)

The registration information on all three eBay accounts lists the **SUBJECT PERSON**’s name, the **SUBJECT PREMISES**, and phone number of (919) 444-4880. Records show phone number (919) 444-4480 is associated with the **SUBJECT PERSON**. The email accounts associated with each account are as follows:

- a. carolina\_otc: olivertwistnc2011@yahoo.com
- b. emily-tastic: olivertwistnc2003@gmail.com
- c. olivertwistnc: olivertwistnc2003@yahoo.com

16. In reviewing eBay transactions associated with the “carolina-otc” account from February of 2020 to February of 2024, investigators discovered over 25,000 items were sold through that account which totaled approximately \$812,611 in revenue. The majority of the items sold consisted of items such as OTC products sold in retail stores.

17. In reviewing eBay transactions associated with the “emily-tastic” account from February 2020 to February 2024, investigators discovered approximately 28,000 items were sold through that account which totaled approximately \$1,024,641 in revenue. The majority of the items sold consisted of retail items such as OTC products sold in retail stores.

18. In reviewing eBay transactions associated with the “olivertwistnc” account from February 2020 to February 2024, investigators discovered approximately 26,000 items were sold through that account which totaled approximately \$942,215 in revenue. The majority of the items sold consisted of items such as OTC products sold in retail stores.

19. A review of some recently listed items (from records obtained directly from eBay) sold on all three of SUBJECT PERSON’s eBay accounts reveals the following transactions:

Account Name	Title of Items Sold	Listing IP Address <sup>1</sup>	Sale Creation Date/Time	Purchase Date/Time
carolina_otc	BOTH BOTTLES of Prevagen Extra Strength AS PICTURED TOTAL OF 60 CAPSULES 2X1102	75.189.129.3	2/1/2024 11:44	2/4/2024 16:25

---

<sup>1</sup> An IP address, or Internet Protocol address, is a unique identification number assigned to a device that is connected to a computer network or the internet.

emily-tastic	Prevagen CHEWABLE EXTRA STRENGTH Mixed Berry flavor 30 Tablets 20mg #1027	75.189.129.3	2/3/2024 6:15	2/6/2024 21:37
olivertwistnc	3 Bottles of Prevagen Professional Strength 30 Capsules Lot of 3 x 30 CT #1010!!	75.189.129.3	1/25/2024 3:06	1/26/2024 14:00

As noted above, all three of the **SUBJECT PERSON**'s eBay account listings were listed using the IP address 75.189.129.3.

20. eBay records additionally show that the **SUBJECT PERSON** has a fourth active eBay account, "Carolina\_DEALS247," that primarily sells sports cards and sports memorabilia. eBay records do show that this account has sold retail products in the past. This account additionally lists the **SUBJECT PREMISES** as the street address on the account registration. Furthermore, records show listings on this account as being associated with the IP address 75.189.129.3.

21. Records show IP address 75.189.129.3 as belonging to Charter Communications, Inc. ("Charter"), a telecommunications company that offers internet, television, and phone services. Charter subscriber records reveal the **SUBJECT PREMISES** as being the physical location linked to IP address 75.189.129.3. Furthermore, Charter records show the subscriber name associated with the IP address as the **SUBJECT PERSON**.

22. According to CVS Pharmacy's Organized Retail Crime and Corporate Investigations (ORCCI), which is a group that monitors online websites and auction sites for the unauthorized selling of products carried by CVS, the **SUBJECT PERSON** is one of the largest sellers of OTC medications who is not an authorized retailer. CVS, Walgreens, Kroger Publix, Harris Teeter, Walmart, etc., are national drugstore chains, and national supermarket chains. An authorized retailer is an individual, business, or legal entity that has been officially appointed by



a manufacturer to sell its products or service. As an example, according to Quincy Biotech, the manufacturer of Prevagen<sup>2</sup>, in order for an entity to legally sell Prevagen, it must be authorized by Quincy Biotech. According to Quincy Biotech, the **SUBJECT PERSON** is not an authorized seller.

23. Additionally, ORCCI representatives advised that national chain retailers are unable to purchase merchandise at the price at which the **SUBJECT PERSON** is selling them. The below chart depicts the price differences between items listed on the **SUBJECT PERSON**'s eBay accounts in comparison to retail prices as of April of 2024:

Retail Product	olivertwistnc Price	Emily-tastic Price	Carolina_otc Price	CVS.com Price	Walgreens.com Price
Prevagen Professional Strength – 30 capsules	_____	\$59.95	_____	\$89.99	\$89.99
Muro 128 5% eye solution- ½ FL Oz	\$18.99	\$18.99	_____	\$36.79	\$36.99
PlanB One-Step- 1.5 mg	\$22.95	_____	\$29.99	\$49.99	\$49.99
Nicorette Gum 2MG- 160 pieces	_____	_____	\$52.99	\$78.49	\$75.99
Rephresh Pro-B- 30 Capsules	\$21.95	\$19.95	_____	\$38.99	\$41.99

24. As of May 7, 2024, all three of the **SUBJECT PERSON**'s eBay accounts had active listings consisting mainly of retail products, including OTC medications. Specifically, the eBay account “olivertwistnc” had 68 products listed for sale; the eBay account “emily-tastic” had 63 products listed for sale; the eBay account “carolina-otc” had 76 products listed for sale.

---

<sup>2</sup> Prevagen is a non-FDA approved over- the-counter dietary supplement sold at various national retailers.

### **C. January 26, 2021, Undercover Purchase**

25. On or about January 26, 2021, the CVS ORCCI Manager made a controlled purchase of Prevagen from the **SUBJECT PERSON**'s eBay site, "olivertwistnc." On January 30, 2021, the Prevagen arrived at its intended destination. The package listed the sender name as the **SUBJECT PERSON** with the return address being the **SUBJECT PREMISES**. The Prevagen's box was checked, and a radio-frequency identification ("RFID")<sup>3</sup> tag was located. The tag was scanned using an RFID scanner and was determined that the original product had been purchased by Food Lion and was intended to be sold on Food Lion shelves, and not through an eBay seller with the username "olivertwistnc."

### **D. Indiana Surveillance**

26. Through the investigation, investigators discovered that numerous large parcels suspected of containing retail merchandise such as OTC products were being mailed from Tina Herwehe's residence located at 5020 Southeastern Avenue, Indianapolis, IN 46203, to the **SUBJECT PREMISES**. Between on or about February 7, 2022, and on or about May 16, 2024, investigators conducted surveillance, through in-person physical observations as well as through the use of a pole camera, at Herwehe's residence. Multiple individuals, both identified and unidentified, were observed bringing large containers, garbage bags, and plastic hand baskets (similar to baskets used at retail stores) filled with what appeared to be product sold by retail stores to Herwehe's Indiana residence. Based on my training and experience, and that of other trained investigators, this activity is consistent with trafficking in stolen merchandise.

---

<sup>3</sup> Prevagen packages are equipped with Radio Frequency Identification, or RFID, tags, which is a security feature used for tracking inventory. RFID scanners can identify a code for the product from Quincy Biotech, the makers of Prevagen, which allows them to identify what company purchased it and what distribution center it was sent to.

27. One of the individuals identified by investigators, Kevin Nichols, was observed arriving to Herwehe's Indiana residence in a Honda Accord on February 8, 2022. Nichols was observed handing a white trash bag containing small boxes to Anthony McKinney and then walking into Herwehe's residence. Investigators then observed Nichols exiting the residence a short time later with cash in his hand and without the white trash bag. Investigators later discovered that on March 2, 2022, Nichols was arrested in Brownsburg, IN, after attempting to steal nine retail products from a CVS store. Law enforcement officers subsequently searched Nichols' Honda Accord that was parked outside the CVS. Officers located and seized 57 retail products from the vehicle, with some of the items still in plastic theft-proof containers called Alpha Keepers or Alpha Boxes (clear plastic containers retailers such as CVS and Walgreens use to help minimize theft of high-value merchandise).

28. On or about March 22, 2022, a trash pull was conducted at Herwehe's residence at 5020 Southeastern Avenue, Indianapolis, IN. In the trash, investigators discovered the same theft prevention alpha box containers which had been opened. None of the alpha boxes appeared to be forcefully opened or damaged. Investigators determined that someone at the residence likely had a key to open the alpha boxes. These keys are usually kept by retailers to open the alpha boxes and access the merchandise for paying customers. The discovery of empty open alpha boxes is highly indicative of product that was stolen inside the alpha boxes. Criminals associated with retail theft will steal alpha boxes containing product, remove the product, then discard the empty alpha boxes. In my training and experience, it can be common for some fences to require boosters to remove all security features such as alpha boxes and security tags prior to shipping the products to the fences. Below is an image of the empty alpha boxes found during the March 22, 2022, trash pull:





29. Between December of 2022 and June of 2023 investigators observed several individuals, on 12 occasions, bringing products in backpacks, red baskets which appeared to be consistent with CVS baskets, and other large bags and containers to Herwehe's residence.

30. While conducting physical surveillance at Herwehe's residence on June 8, 2023, investigators observed Anthony McKinney leaving the residence and traveling to a gas station located at 50 W Thompson Road, Indianapolis, IN 46227. At the gas station, Anthony McKinney met with a white female who arrived in a small sedan. The female carried a large blue plastic bin from her vehicle to the rear of Anthony McKinney's vehicle. Investigators observed Anthony McKinney retrieve a garbage bag and a retail store basket believed to contain retail products from the rear of his vehicle. He was observed sorting through product and placing items into her plastic bin. He then carried the bin to her vehicle and placed it inside the trunk of the vehicle. Investigators then observed the female handing Anthony McKinney cash.



31. On January 30, 2024, investigators conducted a trash pull of Herwehe's residence. The trash pull led to the discovery of seven packages with electronic article surveillance (EAS) tags attached. The tags were tested at a nearby CVS, showing that they were still activated. EAS tags are normally deactivated during a purchase at the cash register. This indicates that the items were not paid for and were not processed through a point of sale.

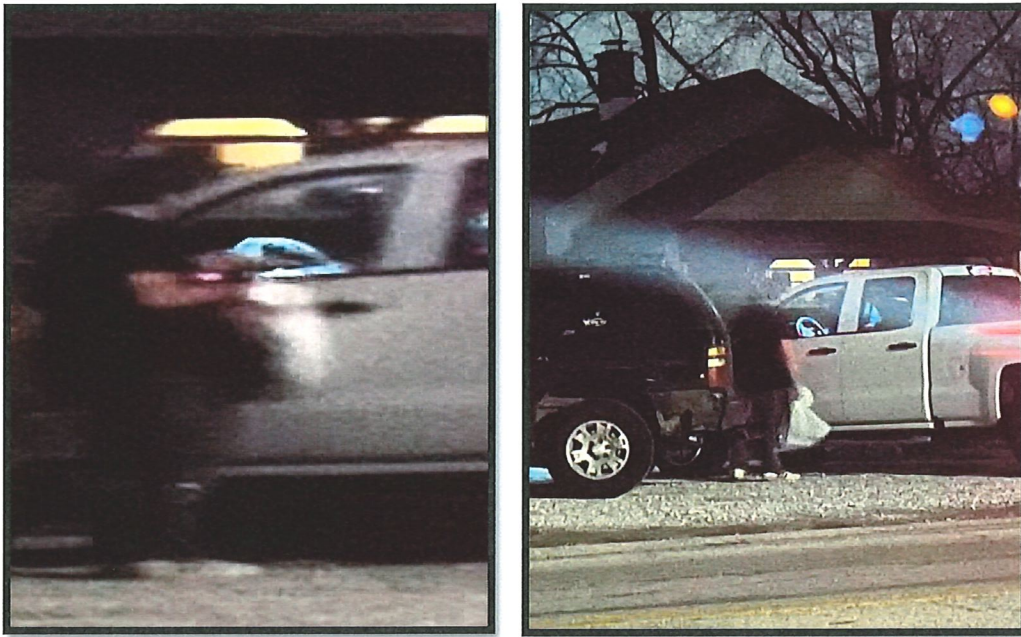


32. On January 31, 2024, at approximately 3:23 p.m., investigators observed Anthony McKinney beside his vehicle removing retail merchandise, including what appeared to be Gillette brand razors and Prilosec OTC medication, from a blue tote. The tote appeared to be the same, or similar, to the blue tote which investigators observed Anthony McKinney using to transfer merchandise believed to be stolen on June 8, 2023. Investigators then observed Anthony McKinney place the items into a box and then enter his residence.



33. On January 31, 2024, at approximately 6:49 p.m., investigators observed a white truck arrive at Herwehe's residence. An unknown male gave Anthony McKinney two white garbage bags from inside of the vehicle. Anthony McKinney and the unknown male spoke for approximately eight minutes. The truck departed and Anthony McKinney was seen taking the white garbage bags into the house.





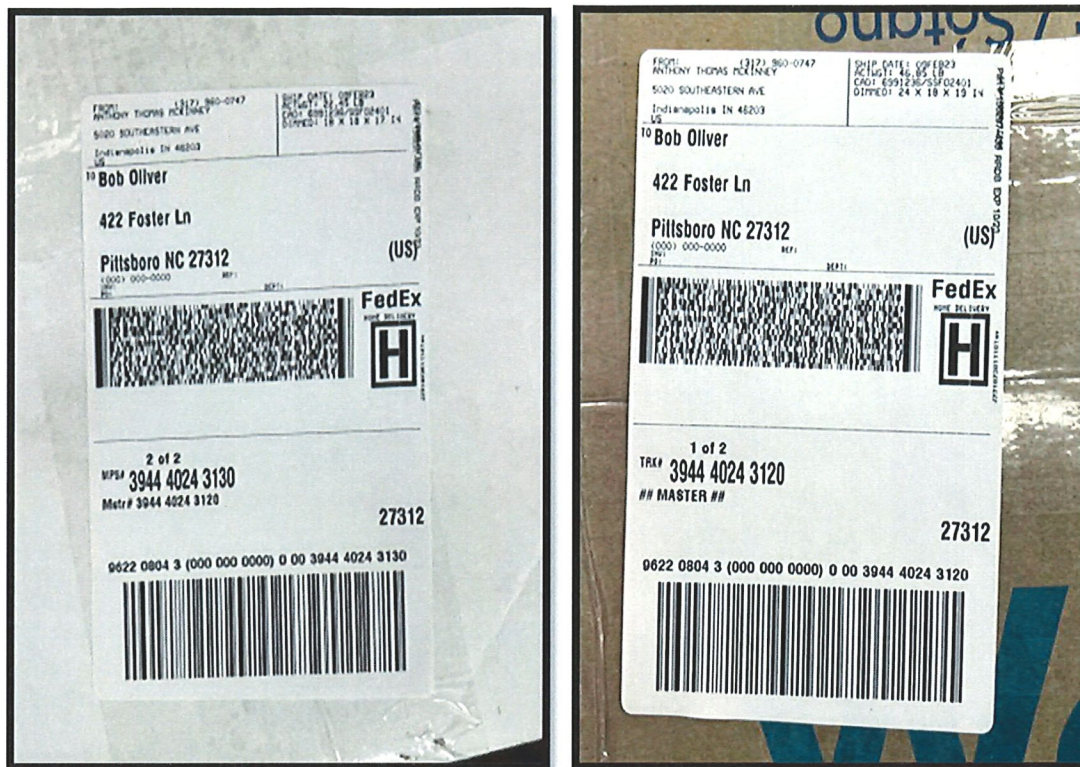
34. On May 15, 2024, investigators observed a second white truck arrive at the residence. An unknown male was seen exiting the vehicle with a white plastic bag and carrying it into the residence. Approximately seven minutes later, the unknown male returned to his vehicle without the white plastic bag and drove off. Based on my training and experience, the instances observed through surveillance, as described above, are likely exchanges of stolen products and payment for them.

**E. FedEx and USPS Shipments Between SUBJECT PREMISES and Herwehe Residence**

35. On February 9, 2023, investigators observed Anthony McKinney carry a large Lowe's box into a vehicle. Investigators followed the vehicle to a FedEx store located at 4155 South East Street, Indianapolis, IN 46227. McKinney was observed carrying the large brown Lowe's box, as well as a large white box, into FedEx. While inside the FedEx store, investigators overheard Anthony McKinney tell the FedEx employee the boxes were going to the **SUBJECT PERSON**. After Anthony McKinney left FedEx, investigators were able to examine the exterior of the boxes. The labels from both boxes had the **SUBJECT PREMISES** listed as the shipping



address. The return address on both labels was, Anthony McKinney, 5020 Southeastern Avenue, Indianapolis, IN.



36. Retail investigators utilized a RFID scanner on the exterior of the boxes and they were able to identify seven units of Prevacen inside the packages. The RFID scan results showed the Prevacen units originated from three different distribution centers. These included a CVS location, a Walgreens location, and a Kroger location. This activity was video recorded and the boxes were not opened or intercepted.

37. According to FedEx records, between August 24, 2020, and October 8, 2022, over 300 FedEx shipments, with an average weight of 29 pounds per parcel, were sent from Anthony McKinney to the **SUBJECT PREMISES**. Based on my training and experience, I am aware that, at times, using shipping services such as FedEx for larger and/or heavier parcels can be more cost-effective than using the USPS. Additionally, based on my training and experience, and the

aforementioned February 9, 2023, FedEx shipment, it is likely that the 300 FedEx shipments from Anthony McKinney to the **SUBJECT PERSON** at the **SUBJECT PREMISES** contains stolen retail products.

38. USPS records show that between March 2022 and February 2024, 25 Priority Mail Express parcels weighing one pound or less, were mailed from the **SUBJECT PERSON** to Herwehe's residence located at 5020 Southeastern Avenue, Indianapolis, IN. One of these parcels, discussed below under the paragraph titled "Parcel 7743," was confirmed to contain thousands of dollars in U.S. currency, and the others are suspected of containing U.S. currency given the similarities in parcel weight and USPS delivery services used. A second parcel identified by postal inspectors, USPS Priority Mail Express parcel bearing USPS tracking number 9481711108033417911744, was sent by the **SUBJECT PERSON** on July 28, 2022, and shipped to Anthony McKinney at his address located at 5020 Southeastern Avenue, Indianapolis, IN. Records show the postage was paid through a STAMPS.COM online postage meter, account number 14406527. The name on the account is listed as the **SUBJECT PERSON** and the address on the account is listed as the **SUBJECT PREMISES**. Furthermore, the email address listed on the account is olivertwistnc2003@yahoo.com, which has been previously discussed in this affidavit as being linked to the **SUBJECT PERSON**.

39. Based on my training and experience, I am aware that Express Mail overnight delivery is intended to be next-day service. The USPS also provides a tracking service through a USPS tracking number, which allows the customer to track the parcel and confirm delivery.

40. Based on my training and experience, and that of other trained investigators, I know that individuals who engage in criminal conspiracies utilize USPS to send and receive items, including money, due to the security of mailing via USPS. I also know that people involved

in criminal activity prefer mail/delivery services such as Express Mail and Priority Mail because of their reliability and the ability to track the article's progress to the intended delivery point. Further, the expedited shipping option makes it easier for individual(s) who mail illegal items and/or illegally obtained money, to circumvent law enforcement detection.

#### **F. USPS Parcel 7743**

41. On or about August 4, 2022, postal inspectors were alerted by the Garfield Post Office in Indianapolis, Indiana of the following parcel addressed to Anthony McKinney, at 5020 Southeastern Avenue, Indianapolis, IN: One USPS Priority Mail Express parcel bearing USPS tracking number 9481 7111 0803 3433 2377 43, addressed to "Anthony McKinney, 5020 Southeastern Ave, Indianapolis IN 46203-3764" with the **SUBJECT PERSON** and **SUBJECT PREMISES** listed as the return address.

42. On August 4, 2022, at approximately 9:37 a.m., postal inspectors retrieved Parcel 7743 from the Garfield Post Office, Indianapolis, IN. On August 8, 2022, postal inspectors applied for a search warrant for Parcel 7743. That application was granted by the Honorable Judge Doris Pryor for the Southern District of Indiana on August 9, 2022 (case number 1:22-mj-0682). On August 9, 2022, the warrant for Parcel 7743 was executed. Contained within Parcel 7743 was \$4,780.00 in U.S. currency. The currency was returned to Parcel 7743, and the parcel was returned to the mail stream in order to continue the investigation.

#### **G. Audio Recordings**

43. On August 4, 2022, an individual identifying himself as Mike Hines, called USPS inquiring about Parcel 7743. In the call, Hines states the package was going to his friend's house on Southeastern Avenue. While on the call, Hines can be heard making another call on a different phone, confirming with an individual he refers to as "Tony" the exact address the



package was going to. “Tony” confirms the address is 5020 Southeastern Avenue. Based on the knowledge of this investigation, inspectors believe Hines was speaking with Anthony McKinney while on the call with USPS. In the call, Hines stated the parcel contained documents and information that they needed.

44. On August 8, 2022, an individual identifying himself as the **SUBJECT PERSON**, calling from 919-444-4880, which is a phone number previously linked to the **SUBJECT PERSON**, called USPS customer service inquiring about Parcel 7743. The **SUBJECT PERSON** stated he sent a guy he knows approximately \$4,000.00 in cash through USPS. In the call, the **SUBJECT PERSON** confirmed Parcel 7743 was picked up from his residence, 422 Foster Ln, Pittsboro, NC 27312, which is the **SUBJECT PREMISES**. In the call, the **SUBJECT PERSON** stated he had wired the guy money before because he is an eBay seller, and the **SUBJECT PERSON** had bought merchandise from him before to resell. Further, on the call, the **SUBJECT PERSON** confirmed his email address was olivertwistnc2003@yahoo.com. Based on the knowledge of this investigation, inspectors believe the individual the **SUBJECT PERSON** was referring to in this call was Anthony McKinney.

45. Based on my training and experience, and that of other postal inspectors who have experience with parcels containing money derived from suspected illicit activities, I know that individuals who call regarding such packages often provide differing stories or variations of the truth as to the contents and/or reason behind the mailing of the package. Because Hines and the **SUBJECT PERSON** gave different explanations as to what was contained in the package, I believe this was an attempt to conceal the nature of the money that was contained in the package.

#### **H. USPS Parcel 8254**

46. On January 26, 2023, postal inspectors were profiling packages going to the **SUBJECT PREMISES** and intercepted a parcel with tracking number 9505511001413024138254 (“Parcel 8254”) that was suspicious in nature. The parcel sounded like it contained pills when moved, and like the boxes shipped to the **SUBJECT PERSON’s** residence in 2019 had a handwritten label and was heavily taped. postal inspectors applied for Federal Search Warrants, and the Honorable United States Magistrate Judge L. Patrick Auld signed the warrant (1:23MJ51).

47. The parcel was opened by postal inspectors pursuant to the signed Federal Search Warrant. The parcel contained the following retail products and name brand OTC medications and some store brand products and OTC medications from CVS and Walgreens.

<u>Items in Box</u>	<u>Quantity</u>
Dermend (Pink)	10
Dermend (Blue)	7
CoQ-10 400 mg	4
Prevagen Extra Strength – Chewable	2
Prevagen Extra Strength – 60 Capsules	3
Prevagen Extra Strength – 30 Capsules	4
Prevagen 30 Capsules	2
RepHresh – Vaginal Probiotic Supplement	3
RepHresh Pro-B Feminine Probiotic Supplement	3
Crest 3D Whitestrips	2
Natural Lamb Luxury Condoms	2
Kardia Mobil	2
Systane Zaditor	6
Muro	10
Super Bata Prostate	5
Ageless Male	3
HClear for him	3
FemiClear	3
FDgard	9
IBgard	9
Mucinex DM	5
Mucinex	2

The parcel was repackaged and placed back in the mail stream for delivery.

## **I. Interview of S.B.**

48. On February 27, 2024, I interviewed a former employee of the **SUBJECT PERSON**, an individual whose initials are S.B. S.B., and other individuals who worked for the **SUBJECT PERSON**, worked at the **SUBJECT PREMISES**. S.B. specifically worked at the **SUBJECT PREMISES** from 2019 to 2022. S.B.'s duties as an employee of the **SUBJECT PERSON** were opening large Lowe's boxes filled with retail products, sorting the items, making sure the expiration dates were still valid, taking photos of the items, and listing the items on eBay. S.B.'s statement of receiving large Lowe's boxes at the **SUBJECT PREMISES** is consistent with investigator's observations of Anthony McKinney shipping out large Lowe's boxes to the **SUBJECT PREMISES** from Indiana.

49. S.B. admitted that the **SUBJECT PERSON** paid S.B. \$25-\$30, in cash, per hour or roughly \$80-\$100 per day. S.B. additionally confirmed that the **SUBJECT PERSON** paid S.B. under the table. According to S.B., the **SUBJECT PERSON** said the cash he was paying S.B. was after taxes were already taken out.

50. The **SUBJECT PERSON** gave S.B. access to his eBay accounts so S.B. could list the items and respond to customers. Once these items would sell on eBay, S.B. would package the items, print shipping labels, and ship the items out from the **SUBJECT PREMISES** via the USPS. S.B. believed the USPS would pick up between 150 to 200 packages a day from the **SUBJECT PREMISES**.

51. USPS records show that in 2022 and 2023, the **SUBJECT PERSON** shipped out over 28,000 parcels from **SUBJECT PREMISES** through the USPS.

52. The **SUBJECT PERSON** told S.B. that he purchased the items at discounted prices from stores that went out of business. These items included merchandise that would



originally be sold at grocery stores like Wal-Mart and retail stores like CVS, and included health and beauty items, vitamins, condoms, make-up, and over-the-counter medications. The **SUBJECT PERSON** additionally instructed S.B. to remove any security sticker tags that were found on some of the items before listing them for sale. S.B. also noticed many of the items were shipped to the **SUBJECT PERSON** with security tags already damaged. When asked why the **SUBJECT PERSON** had S.B. take off the security stickers, S.B. said that the **SUBJECT PERSON** stated that he did not want the items to look damaged when posting photos of the items on eBay.

53. While working for the **SUBJECT PERSON**, S.B. recalled seeing numerous items encased in Alpha Box security containers. Specifically, S.B. stated that those particular cases were placed on a shelf inside the **SUBJECT PREMISES**. As previously mentioned in this affidavit, alpha boxes are security containers used by retailers to minimize theft of high-value merchandise and require a special key to open them.

54. To figure out the listing price for each item sold through the **SUBJECT PERSON's** eBay accounts, the **SUBJECT PERSON** requested that S.B. research prices online for each particular item. The **SUBJECT PERSON** maintained a spreadsheet for the inventory which listed the cost of the item, the profit the **SUBJECT PERSON** wanted to make off each item, and the listing price. All of the **SUBJECT PERSON's** employees had laptops that were collectively synced together so that employees could access the main pricing spreadsheet. When asked who added the cost or price paid for each item to the spreadsheet, S.B. stated that the **SUBJECT PERSON** somehow added the cost of each item to the spreadsheet prior to the employees inventorying and entering each item onto the spreadsheet. S.B. confirmed that the **SUBJECT PERSON** had his own desktop computer that he primarily used. S.B. believed that

the **SUBJECT PERSON** had numerous desktop computers that he used. S.B. additionally told investigators that the **SUBJECT PERSON** owned multiple cellular telephones and would send emails and text messages related to the **SUBJECT BUSINESSES** from his cell phones. From memory, S.B. recalled the **SUBJECT PERSON**'s phone number as being (919) 444-0880, which is one digit off from the **SUBJECT PERSON**'s actual number of (919) 444-4880. A check of the phone number provided by S.B., (919) 444-0880, shows that it is not registered to anyone. In my training and experience, given the similarity between both phone numbers, S.B. attempting to recall the number by memory, and the number provided by S.B. as not being a registered number, it is likely that S.B. was attempting to recall the **SUBJECT PERSON**'s actual phone number (919) 444-4880.

55. According to S.B., the **SUBJECT PERSON** would send cash payments, via USPS Express Mail, to individuals who sold him the bulk merchandise. S.B. also recalled the **SUBJECT PERSON** repeatedly going to Navy Federal Credit Union to send individuals money.

56. S.B. stated that the **SUBJECT PERSON** primarily used three email addresses to conduct business and recalled one of them as being olivertwistnc2003@gmail.com.

**J. olivertwistnc2003@gmail.com Records**

57. Gmail subscriber records associated with the email address olivertwistnc2003@gmail.com, which has previously been identified in this affidavit as being linked to the **SUBJECT PERSON**'s eBay account "emily-tastic" and also identified through S.B.'s interview, shows the account registered to the name "Bob" with no last name listed. The account was created by the **SUBJECT PERSON** in September of 2009.

58. The Google Pay billing account associated with olivertwistnc2003@gmail.com lists the customer name of “Bob Oliver,” which is a name the **SUBJECT PERSON** commonly used, and the address as the **SUBJECT PREMISES**.

59. Login activity for this Gmail account identifies the IP address of 75.189.129.3 as logging into the account as recently as January 22, 2024. As previously discussed in this affidavit, IP address 75.189.129.3 has been linked to the **SUBJECT PERSON** at the **SUBJECT PREMISES**.

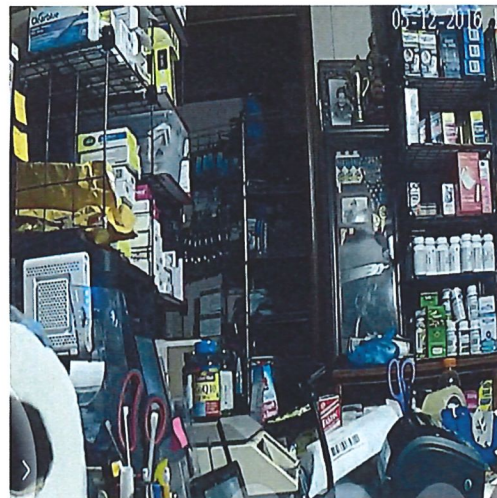
60. postal inspectors applied for a Federal Search Warrant on the email address, olivertwistnc2003@gmail.com, and the Honorable Joe L. Webster signed the warrant (1:24MJ186-1). Investigators subsequently obtained records on the account and reviewed photographs, videos, and screenshot images from what appeared to be a cellular telephone associated with the account. The following photographs and images were discovered:

- a. An image of a USPS Priority Mail Express label with the return address of the **SUBJECT PERSON** at the **SUBJECT ADDRESS** addressed to “T MCKINNEY, 5020 SOUTHEASTERN AVE., INDIANAPOLIS, IN 46203”. The label listed a scheduled delivery date of August 27, 2021.
- b. Images of several handwritten and typed inventory and pricing sheets which contained the names of numerous OTC medications, quantity of items, and price per item.
- c. One image containing four boxes of KardiaMobile, which is a device sold at retail stores that can record electrocardiograms, with damaged and removed EAS security stickers.



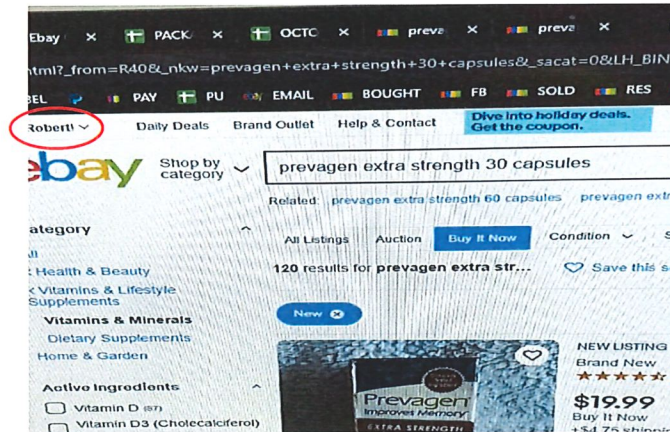
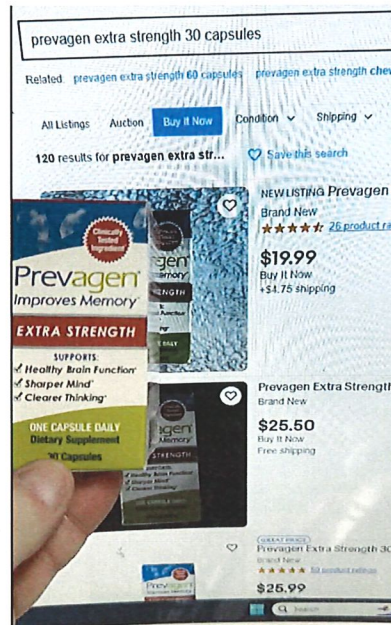


- d. Images from inside the residence believed to be the **SUBJECT PREMISES** of shelving containing a large quantity of shipping boxes and containers, packaging material, and retail products and OTC medication. These images are consistent with statements made by S.B., and others, who have been inside the **SUBJECT PREMISES**.

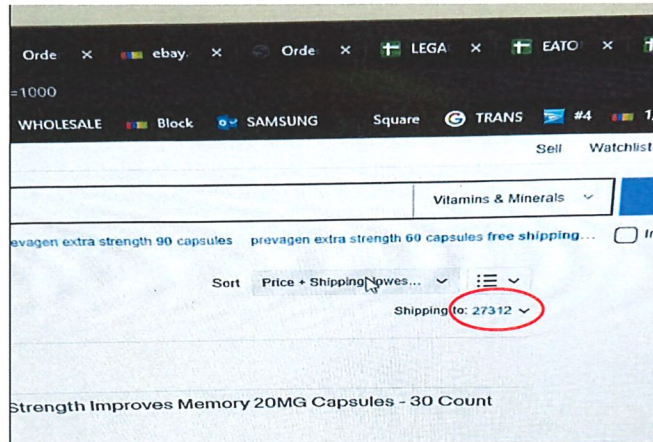


- e. A tutorial video made by the **SUBJECT PERSON** on how to obtain the current pricing on eBay of Prevagen Extra Strength 30 capsules. On the video, the **SUBJECT PERSON** is recording himself on a computer navigating several eBay sites and

discussing tips on selling Prevagen on eBay and the best methods to find accurate pricing. The eBay homepage on the computer screen displays the name “Robert” and indicates “Shipping to: 27312”, which is the same zip code as the **SUBJECT PREMISES** (highlighted in red on screenshots below).







f. Cellular telephone screenshot images of text messages discussing the purchase and sale of retail products and OTC medications as well as shipping and payment records.

61. The recovery telephone listed on the account is the **SUBJECT PERSON**'s phone number (919) 444-4880. Furthermore, the alternate e-mail address and recovery email address listed on the Gmail account is olivertwistnc2003@yahoo.com.

#### K. olivertwistnc2003@yahoo.com Records

62. Yahoo subscriber records associated with the email address olivertwistnc2003@yahoo.com, which has previously been identified in this affidavit as being linked to the **SUBJECT PERSON**'s eBay account "olivertwistnc" and also identified as the email address the **SUBJECT PERSON** provided on his call to USPS customer service on August 8, 2022, shows the registered name on the account as the **SUBJECT PERSON** in the city of "Pittsboro, NC 27312." The account registration date is listed as January 1, 2005. The recovery phone number on the account is (919) 444-4880, which has previously been discussed in this affidavit as being linked to the **SUBJECT PERSON**.

63. The email address olivertwistnc2003@yahoo.com is listed as a recovery email for another one of the **SUBJECT PERSON**'s yahoo accounts, olivertwistnc2011@yahoo.com,



which is the email address linked to the **SUBJECT PERSON**'s third eBay account, "carolina\_otc".

64. Login activity for olivertwistnc2003@yahoo.com account identifies the same IP address linked to the **SUBJECT PERSON** at the **SUBJECT PREMISES**, 75.189.129.3, as logging into the account as recently as February 4, 2024. Furthermore, Charter subscriber records associated with the IP address 75.189.129.3 show that olivertwistnc2003@yahoo.com is one of the email accounts listed under "User Name or Features" on the account.

65. Bank of America records show that on May 28, 2021 and on October 12, 2021, the **SUBJECT PERSON** listed the email address olivertwistnc2003@yahoo.com on two business credit card applications for the corporation named "CAROLINA DEALS247", which is the same name as one of the **SUBJECT PERSON**'s active eBay accounts.

#### **L. February 27, 2024, Undercover Purchase**

66. On or about February 27, 2024, the CVS ORCCI Manager made a controlled purchase of Prevagen from **SUBJECT PERSON**'s eBay site, "carolina\_otc." On March 1, 2024, the Prevagen arrived at its intended destination. The package listed the sender name as the **SUBJECT PERSON** with the return address being the **SUBJECT PREMISES**. The Prevagen box was checked, and an RFID tag was located. The tag was scanned using an RFID scanner and it was determined that the original product had been purchased by CVS and was intended to be sold on CVS shelves, and not through an eBay seller with the username "carolina\_otc".

#### **M. USPS Parcel 5144 & USPS Parcel 5168**

67. On February 28, 2024, postal inspectors were profiling packages going to the **SUBJECT PREMISES** and intercepted two parcels, with tracking numbers 9534 6105 5363 4057 7551 44 ("Parcel 5144") and 9534 6105 5363 4057 7551 68 ("Parcel 5168"), that were

suspicious in nature. Both parcels sounded like they contained pills when moved, and like the boxes shipped to the **SUBJECT PREMISES** in 2019 and 2023, had handwritten labels and were heavily taped. Both parcels had handwritten labels with the sender name, “Redick,” with a return address of 2018 Oldfield Pt. Rd., Elkton, MD.

68. Postal inspectors applied for Federal Search Warrants, and the Honorable United States Magistrate Judge Joe. L Webster signed the warrants (1:24MJ92-1 and 1:24MJ93-2) on February 28, 2024. On February 29, 2024, both parcels were opened by postal inspectors in Greensboro, NC, pursuant to the signed Federal Search Warrant. Both parcels contained 144 OTC medications and retail items.

69. Parcel 5144 contained the following items:

<u>Items in Box</u>	<u>Quantity</u>
Prevagen (30 Capsules- Professional Formula)	4
Prevagen (30 Capsules- Extra Strength)	6
Prevagen (30 Capsules- Regular Strength)	6
Plan B One-Step	16
Inventory Sheet (containing list of OTC items, from both parcel 5144 & parcel 5168, quantity of each item, price per unit of each item, and totals)	1

After closely inspecting each item, I discovered that all of the Prevagen packages had small cuts across the front of the packaging. Upon turning each Prevagen package over, it was evident that the cuts were made through each of the package’s Electronic Article Surveillance (EAS) anti-theft sticker tags (as diagramed in the below pictures within the red highlighted area).



70. In my training and experience, I know that retailers use EAS stickers as a theft prevention system. When a paying customer presents an item with an EAS sticker at a point of sale (POS) register, the EAS sticker is disabled after payment is made, allowing the paying customer to walk-out of the store without the security pedestals or alarms being activated. Thieves can circumvent the security pedestals from being activated by cutting the EAS stickers or removing them from the packaging altogether, thus making the EAS stickers ineffective in activating any security alarms.

71. I used the RFID Prevagen scanner to scan 16 Prevagen bottles located inside of one of the parcels. The results of those scans show that all 16 Prevagen bottles were initially slated to be sold at Walgreens.

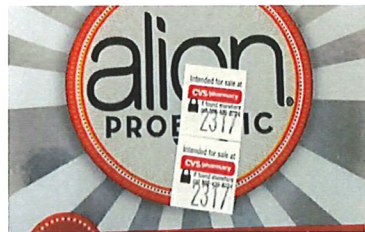
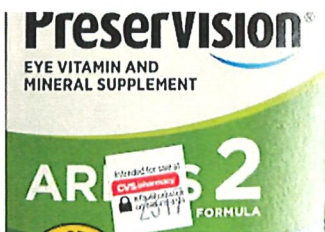
72. Parcel 5168 contained the following items:

<u>Items in Box</u>	<u>Quantity</u>
PreserVision Areds120	2
Preservision Areds 130	1
RePhresh Pro-B	9
Florastor	5



IB Gard	28
FD Gard	13
AZO	8
Muro Eye Ointment	14
Dermed- Pink	5
Dermed- Blue	4
Recticare	3
Flonase Sensimist	3
Crest Glamorous Whitening Strips	3
Crest 1-hour express Whitening Strips	2
Zyrtec 90	19
Zyrtec 60	5
Align 56	3
Align 42	16
Allergy Test kit	1

73. I also discovered two packages of PreserVision, three packages of Align Probiotic, and two packages of RectiCare with stickers that contained the following statement, “Intended for Sale at CVS/pharmacy if found elsewhere call 866-439-8724.”



74. A manager with CVS’s ORCSI confirmed that these stickers were placed onto these items by CVS employees and the items were intended to be sold at CVS retail stores only.

75. Furthermore, when asked what happens to remaining retail merchandise, such as OTC medications, at a CVS store that goes out of business or permanently closes, CVS’s ORCSI manager stated that the items would be shipped to another CVS store and sold there. The ORCSI manager confirmed that these items would never be sold, in bulk, to the **SUBJECT PERSON** outside of a retail setting. Additionally, CVS’s ORCSI group queried all incoming phone calls to the 866-439-8724 number to determine if anyone had called CVS to report the missing containers

of PreserVision and/or Align Probiotics. The ORCSI group found that no calls were received from the **SUBJECT PERSON** between March of 2021 to March of 2024.

76. As previously mentioned in this affidavit, both parcels had handwritten labels with the sender name, "Redick," with a return address of 2018 Oldfield Pt. Rd., Elkton, MD. Investigators identified Richard Redick as an individual currently living at that address. A criminal history check on Redick reveals that has been previously arrested for theft of retail items, to include at least one incident involving the theft of retail merchandise similar to the items found in the 2019, 2023, and 2024 parcels. Additionally, USPS records show that within the last five months (between October of 2023 and February of 2024), there have been 10 parcels weighing between 5 to 20 pounds originating from Redick OR Elkton, MD being shipped to the **SUBJECT PREMISES**.

77. On February 29, 2024, both parcels were repackaged by postal inspectors and handed to a USPS employee in Pittsboro, NC, to be delivered. The USPS employee subsequently traveled to the **SUBJECT PREMISES** and placed both items inside a room of the residence that is commonly used for parcel deliveries.

78. In continued profiling of USPS packages being shipped to the **SUBJECT PREMISES**, investigators discovered that between the dates of March 1, 2024, and April 26, 2024, the **SUBJECT PERSON** has received seven parcels weighing over five pounds at the **SUBJECT PREMISES**. In my training and experience, the weight and shipping services associated with these parcels are consistent with previous parcels shipped to the **SUBJECT PREMISES** that were verified to contain retail merchandise. Given the above-mentioned statements from witnesses, eBay records, and shipment records, it is likely that retail products, such as OTC medications, are currently located inside **SUBJECT PREMISES**.

#### **N. Confidential Source Interview**

79. On February 29, 2024, I interviewed a confidential source, an individual whose initials are L.B., who regularly meets with the **SUBJECT PERSON** and frequents the **SUBJECT PREMISES**. L.B. advised that in early February of 2024, L.B. entered the **SUBJECT PREMISES** and observed over 1000 retail products on shelves that included pregnancy tests, allergy medications, and dog medications. L.B. additionally stated that the **SUBJECT PERSON** had openly discussed receiving a parcel at the **SUBJECT PREMISES** that contained OTC medication returned by a customer.

#### **O. May 30, 2024, Undercover Purchase**

80. On or about May 30, 2024, the CVS ORCCI Manager made a controlled purchase of Prevagen from the **SUBJECT PERSON**'s eBay site, "emily\_tastic." On May 31, 2024, postal inspectors intercepted all outbound parcels originating from the **SUBJECT PREMISES**. Postal inspectors discovered 49 parcels packaged in white mailer envelopes or small boxes. While handling the parcels, postal inspectors noted that most of the parcels sounded like they contained pills. All the parcels had shipping labels with pre-paid postage and the **SUBJECT PREMISES** listed as the return address. While all the parcels bore the **SUBJECT PREMISES** as the return address, they all contained the following names associated with the return address, "Emily Tastic", "Bob Oliver", "Carolina\_OTC", "olivertwistnc", and "Robert W Oliver". The business names are the same names associated with the **SUBJECT PERSON**'s eBay accounts. In my training and experience, individuals who ship numerous items daily using prepaid postage bearing different business names on the labels usually operate multiple businesses or entities from the same location. Below are images of the outbound parcels being shipped from the **SUBJECT PREMISES** on May 31, 2024.





81. Postal inspectors retrieved the parcel associated with the May 30, 2024, controlled purchase. The package listed the sender name as the **SUBJECT PERSON** with the return address being the **SUBJECT PREMISES**. On June 3, 2024, postal inspectors opened the parcel and discovered a bottle of Prevagan matching the item description listing on the **SUBJECT PERSON**'s eBay site, "emily\_tastic."

**P. PayPal Account XXX XXXX XXXX XXXX 7490**

82. A review of PayPal transaction records between the dates of January 2019 and February 2024, for account ending 7490, show it to be an account registered to the **SUBJECT PERSON** at the **SUBJECT PREMISES**. Financial transactions on account 7490 show that this PayPal account is funded, in part, through the sale of OTC products and retail merchandise. Between the dates of January 1, 2019, and February 2024, PayPal account 7490 received approximately \$1,263,401 in incoming payments.

83. Records additionally show Bank of America checking accounts ending 2752 and 9725, which were opened by the **SUBJECT PERSON**, are banks accounts currently linked to PayPal account 7490 as of February 2024.

**Q. PayPal Account XXX XXXX XXXX XXXX 9287**

84. A review of PayPal transaction records between the dates of January 2019 and February 2024, for account ending 9287, show it to be an account registered to the **SUBJECT PERSON** at the **SUBJECT PREMISES**. Additionally, the primary email account associated with the PayPal account ending in 9287 is listed as olivertwistnc2003@yahoo.com. Financial transactions on account 9287 show that this PayPal account is funded, in part, through the sale of OTC products and retail. Between the dates of January 1, 2019, and February 2024, PayPal account 9287 received approximately \$5,498,109 in incoming payments.

85. PayPal records for account ending 9287 additionally show numerous payments made to S.B. Specifically, between December 2020 and January 2021, 25 payments totaling \$5,235 were made directly to the counterparty name of S.B. in the form of "Mobile Payments-Personal" as well as "General Payments- Personal". Additionally, one payment for \$2,750 was made on April 2, 2021, with the payment notes reflecting April rent for S.B.

86. PayPal records additionally show Bank of America checking accounts ending 2752, 9725, and 4334, which were opened by the **SUBJECT PERSON**, are current bank accounts linked to PayPal account 9287 as of February 2024.

**R. Bank of America Account XXXXX2752**

87. Investigators reviewed Bank of America account ending 2752, which was opened by the **SUBJECT PERSON**. The address on the account statement is listed as the **SUBJECT PREMISES**. Investigators discovered that between on or about January 1, 2019, and on or about

February 2024, BOA account ending 2752 was one of three BOA accounts controlled by the **SUBJECT PERSON** that was receiving funds from PayPal and eBay which investigators believe to be related to the sale of retail products from the **SUBJECT PERSON's** aforementioned eBay business accounts.

88. Specifically, between January 20, 2021, and July 22, 2022, eBay Seller Payout records for the **SUBJECT BUSINESSES** show the following transfers being made into the Bank of America account ending 2752:

<u>eBay Account</u>	<u>Transfer Amount</u>
Carolina_otc:	\$315,906.51
Emily-tastic:	\$528,301.84
Olivertwistnc:	<u>\$191,891.39</u>
<b>Total:</b>	<b>\$1,036,099.74</b>

89. Records from BOA account ending 2752 additionally show that between January 9, 2019, and May 17, 2022, over 130 wire transfers totaling \$517,308 were sent by the **SUBJECT PERSON** to Herwehe and McKinney. Many of the wire transfers were performed one to four days apart from each other and none of the transfers were over \$10,000. In my training and experience, individuals who repeatedly send out large wire transfers under \$10,000 to the same individual, within a short period of time, do so to avoid scrutiny from financial institutions and to evade law enforcement.

90. A review of other outbound payments on BOA account ending 2752 additionally revealed hundreds of Peer to Peer (“P2P”)<sup>4</sup> payments (from payment processing companies such as CashApp, Zelle, and FB Pay) to several known and unknown individuals. These outbound payments consisted of amounts that varied from ten dollars to two thousand dollars. Many of

---

<sup>4</sup> Peer to Peer (“P2P”) payment services are financial transactions made between two parties with separate bank accounts, provided by a third-party website or mobile application.



these payments were sent by the **SUBJECT PERSON** to the same recipients within a timespan of several days. In my training and experience, individuals who repeatedly send multiple P2P payments, within a short period of time to the same individual, do so to avoid law enforcement detection.

**S. Bank of America Account XXXX XXXX 4334**

91. Investigators reviewed Bank of America account ending 4334, which was opened by the **SUBJECT PERSON**. The address on the account statements is listed as the **SUBJECT PREMISES**. Investigators confirmed that account 4334 was identified as receiving funds from PayPal and eBay which investigators believe to be related to the aforementioned sale of OTC products from the **SUBJECT BUSINESSES**.

92. Between July 22, 2022, and May 18, 2024, eBay Seller Payout records for the **SUBJECT BUSINESSES** show the following transfers being made into the Bank of America account ending 4334:

<u>eBay Account</u>	<u>Transfer Amount</u>
Carolina otc :	\$374,314.77
Emily-tastic:	\$334,700.80
Olivertwistnc:	<u>\$256,306.19</u>
<b>Total:</b>	<b>\$965,321.76</b>

93. A review of outbound payments on BOA account ending 4334 revealed numerous P2P payments that were sent by the **SUBJECT PERSON** to the same recipients within a timespan of several days.

**T. Bank of America Account XXXX XXXX 9725**

94. Investigators reviewed Bank of America account ending 9725, which was opened by the **SUBJECT PERSON**. The address on the account statements is listed as the **SUBJECT RESIDENCE**. Investigators confirmed that account 9725 was identified as receiving funds from

PayPal and eBay which investigators believe to be related to the aforementioned sale of OTC products from the SUBJECT BUSINESSES.

95. A review of outbound payments on BOA account ending 9725 also revealed numerous P2P payments that were sent by OLIVER to the same recipients within a timespan of several days.

96. Bank records additionally reveal that between January 2022 and January 2024, the **SUBJECT PERSON** conducted hundreds of online bank transfers ranging from \$100 to several thousand dollars between all three of the **SUBJECT PERSON's** BOA accounts. These records show multiple transfers made to and from the same accounts on an almost weekly basis. In my training and experience, individuals who conduct numerous transfers between multiple accounts of the same financial institution, also known as layering<sup>5</sup>, do so in an effort to make the source of those funds difficult to trace.

97. Additionally, BOA records show the **SUBJECT PERSON** conducting large ATM cash withdrawals between all three accounts with similar frequency. Below is a table reflecting ATM withdrawals across all three BOA in the 12-day period between July 7, 2022, and July 18, 2022.

BOA CHATHAM CROSSING- CHAPEL HILL, NC				BOA RESEARCH TRIANGLE PARK, DURHAM, NC			
TRANS. DATE	ACCT 2752	ACCT 4334	ACCT 9725	TRANS. DATE	ACCT 2752	ACCT 4334	ACCT 9725
7/7/2022	\$800.00	\$800.00	\$800.00				
	\$700.00		\$700.00				
				7/8/2022	\$800.00	\$800.00	\$800.00
					\$700.00		\$700.00
7/9/2022	\$800.00	\$800.00	\$800.00				
	\$700.00		\$700.00				

---

<sup>5</sup> According to the U.S. Department of Treasury, layering involves separating the illegally obtained money from its criminal source by layering it through a series of financial transactions, which makes it difficult to trace the money back to its original source.

7/11/2022		\$1,200.00	\$800.00				
		\$1,200.00	\$700.00				
7/12/2022		\$1,200.00	\$800.00				
		\$1,200.00	\$700.00				
		\$100.00					
7/14/2022	\$1,200.00	\$1,200.00	\$1,200.00				
	\$300.00	\$1,200.00	\$300.00				
		\$100.00					
7/15/2022	\$1,200.00	\$1,200.00	\$1,200.00				
	\$300.00	\$1,200.00	\$100.00				
		\$100.00					
7/17/2022	\$800.00	\$1,200.00	\$1,200.00				
	\$700.00	\$1,200.00	\$300.00				
		\$100.00					
7/18/2022	\$1,200.00	\$1,200.00	\$1,200.00				
	\$300.00	\$1,200.00	\$300.00				
		\$100.00					

The above table shows a total of \$41,100 cash withdrawn from two ATM locations for this 12-day period. Specifically, the activity shows multiple ATM withdrawals from all three accounts on the same day. In my training and experience, individuals who conduct multiple ATM withdrawals on a recurrent basis from multiple accounts, all within the same day, are attempting to structure cash withdrawals in an effort to evade detection by law enforcement. Additionally, in my training and experience, these cash withdrawals are also consistent with the **SUBJECT PERSON** obtaining cash to mail cash payments to Herwehe, and others, as previously discussed in this affidavit.

**THERE IS PROBABLE CAUSE TO BELIEVE THAT RECORDS AND ITEMS  
RELATING TO THE PURCHASE AND SALE OF STOLEN RETAIL MERCHANDISE  
WILL BE FOUND AT THE SUBJECT PREMISES**

98. Records from the NC Department of the Secretary of State for one of the **SUBJECT PERSON's** businesses, "Carolina\_deals247 LLC," list the **SUBJECT PREMISES** as the principal address of the business. The articles of incorporation were signed June 17, 2022, by "Robert Oliver Member/Organizer."



99. State law enforcement database records show the **SUBJECT PERSON** has an active North Carolina driver's license. The driver's license issued April 14, 2023, reflects the **SUBJECT PREMISES** as the address for the **SUBJECT PERSON**.

100. Based upon my training and experience, and witness statements, when individuals receive a large quantity of goods, such as the **SUBJECT PERSON** does at the **SUBJECT PREMISES**, in an attempt to sell those goods at higher prices on platforms such as eBay, they must physically store those items and have them readily available to ship when they sell. I know that the **SUBJECT PERSON** has three active eBay accounts with numerous retail items currently listed for sale. I also know that the **SUBJECT PERSON** has received shipments of retail products that still contain theft-prevention devices such as EAS stickers. Witness statements also reveal that anti-theft devices, such as Alpha Boxes, have been stored inside of the **SUBJECT PREMISES**. It is highly likely that stolen retail merchandise and theft-prevention devices will be found in the **SUBJECT PREMISES**.

101. Based on my training and experience, it is likely that electronic devices and/or computers, such as laptop computers, desktop computers, tablets, smart phones, and other digital media means used to access the internet in order to conduct eBay transactions, communicate with customers and retail merchandise suppliers, and conduct P2P payments and wire transfers, as previously mentioned, are maintained on the **SUBJECT PREMISES** or on the **SUBJECT PERSON**.

102. It is also likely that electronic devices and/or computers containing IP address information and other digital records associated with the previously mentioned records are maintained at the **SUBJECT PREMISES**, which is the physical location associated with the device linked to the subscriber IP address of 75.189.129.3.

103. Furthermore, based upon my training, experience, and participation in investigations involving violations of financial crimes and related offenses, and my discussions with investigators involved in similar investigations, I know that individuals who conduct these types of schemes maintain records related to the payment of stolen retail merchandise, invoices, shipment records, and financial institution data at their residence or residences linked to the fraud. Such records would include bank statements, spreadsheets, check stubs, checks, deposit slips, payment records, shipping invoices and packaging materials, correspondence with merchants and others, emails, faxes, letterheads, and credit card files. These records can be maintained in paper form or electronically filed on laptops, smartphones, and other digital storage devices.

#### **SUMMARY OF PROBABLE CAUSE**

104. Based on the above, the investigation has determined that the **SUBJECT PERSON** is likely engaged in the business of obtaining stolen merchandise such as OTC medications and retail products and then reselling the items through online retailers such as eBay. Based on the **SUBJECT PERSON's** financial records and other connections to suspected shoplifting rings, as well as the fact that he sells the products well below market retail value, despite not being an authorized dealer, it is believed that the majority of merchandise the **SUBJECT PERSON** is selling through online retailers is stolen.

105. The investigation has further revealed that stolen merchandise is shipped to the **SUBJECT PREMISES** usually through the US Mail, FedEx, and/or United Parcel Service and is stored at the **SUBJECT PREMISES** before being sold. When the **SUBJECT PERSON** sells the items through eBay, he uses the United States Postal Service primarily, or else he relies on FedEx and United Parcel Service to ship the items to the buyer.

106. Additionally, based on my training and experience, individuals, such as the **SUBJECT PERSON**, who utilize numerous payment methods, and parcel out those payments within a short timeframe to stay under the \$10,000 reporting requirement, are attempting to knowingly launder proceeds from funds obtained through fraudulent means, which in this investigation, is generated from the sales of stolen retail products.

#### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

107. As described in Attachment B, this application seeks permission to search for records that might be found on the **SUBJECT PREMISES**, identified in Attachment A , and in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

108. I submit that if a computer or storage medium is found on the **SUBJECT PREMISES**, there is probable cause to believe records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and guidance from Computer Forensic Analysts with the United States Postal Inspection Service, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file



on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space — that is, in space on the storage medium that is not currently being used by an active file — for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

109. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose

of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the **SUBJECT PREMISES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium, but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and “chat” programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. (A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.) This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. Registry information, configuration files, user profiles, e-mail, e-mail address books,

“chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus



programs (and associated data) may be relevant to establishing the user's intent.

110. In most cases, a thorough search of the premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy known as a mirror image of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on the premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and

configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

111. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

112. It is possible that the **SUBJECT PREMISES** will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

### **PROCEDURE FOR UNLOCKING ENCRYPTED DEVICES**

113. The search warrant requests authorization to use the biometric unlock features of a device (including phones and computers), as described in Attachment B, based on the following, which I know from my training, experience, and review of publicly available materials:

- a. Users may enable a biometric unlock function on some digital devices (including phones and computers). To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.
- b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

114. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of



the warrant: (1) depress Robert OLIVERS' thumb and/or fingers on the device(s); and (2) hold the device(s) in front of Robert OLIVERS' face with his eyes open to activate the facial-, iris- and/or retina-recognition feature.

### CONCLUSION

115. Based upon my training and experience and the investigation described above, I submit that there is probable cause to believe that the **SUBJECT PERSON** has violated the criminal statutes listed above and that evidence, fruits, and instrumentalities of these crimes as described in Attachment B are contained within the **SUBJECT PREMISES** described in Attachments A.

116. I, therefore, respectfully request that the attached warrant be issued authorizing the search of the **SUBJECT PREMISES** and the seizure of the items listed in Attachment B to include a full forensic examination of any computers, electronics, and related devices listed here.

Respectfully submitted,

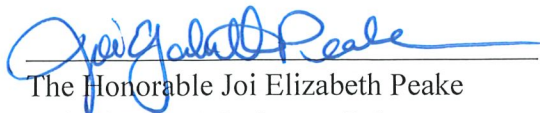
/s/ Alberto G. Sanabria

Alberto G. Sanabria

Postal Inspector

United States Postal Inspection Service

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 5 day of June, 2024, at 6:04 a.m./p.m.



The Honorable Joi Elizabeth Peake  
United States Magistrate Judge  
Middle District of North Carolina

## ATTACHMENT A

### **Property to Be Searched**

This warrant applies to items and information associated with the **SUBJECT PREMISES**, 422 FOSTER LANE, PITTSBORO, NC 27312, including the residence, any outbuildings, and/or other structures within the property's curtilage, and any appurtenances thereto (all of which constitute the **SUBJECT PREMISES**).

The **SUBJECT PREMISES** can be further described as:

A single-story home with cream-colored siding, red brick foundation, and brown-colored roof. The front of the home has five windows with dark-colored shutters. The front door is located in a small, enclosed porch that has wooden steps and railing.

A photograph of the **SUBJECT PREMISES** is below:



## **ATTACHMENT B**

### **Items at Premises to be Seized by the Government**

This Warrant authorizes agents with the United States Postal Inspection Service, assisted by any Federal, State, or local law enforcement agencies deemed necessary, to search the entire **SUBJECT PREMISES**, including the residence, any outbuildings, and/or other structures within the property's curtilage, and any appurtenances thereto (all which constitute the **SUBJECT PREMISES**) identified in Attachment A for evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 2314 (interstate transportation of stolen property), 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1349 (conspiracy to commit mail and wire fraud), and 18 U.S.C. § 1956 (money laundering) (**SUBJECT OFFENSES**) involving Robert ("Bob") Oliver (**SUBJECT PERSON**), and others in the form of:

- a. Any and all stolen property, including but not limited to OTC nonprescription drugs and medical devices that are approved by the FDA, non-FDA approved products such as vitamins, minerals, dietary, and health supplements, personal care products, pet medications, and other retail products from commercial retailers, national drugstore chains, and national supermarket chains, such as CVS, Kroger, Harris Teeter, Publix, Target, Walmart, and Walgreens, etc. (collectively "**STOLEN PRODUCT**");
- b. Any and all security/theft over-ride devices or other devices that aid in the theft or removal of property from commercial retailers, national drugstore chains, and national supermarket chains, such as CVS, Kroger, Target, Publix, Harris Teeter, Walmart, and Walgreens, etc., without consent of the retail store;



- c. Any and all devices, tools and instruments that either remove or aid in the removal of individual retailers identifying markings and/or stickers;
- d. Any and all theft prevention devices, such as Alpha Keepers and Alpha Boxes, used by retailers to prevent the theft of high-value retail items;
- e. Any and all items used to store and/or conceal **STOLEN PRODUCT**;
- f. Any and all correspondence with boosters and/or fences regarding obtaining and selling **STOLEN PRODUCT**;
- g. Any and all financial records and financial information relating to the **SUBJECT PERSON** and the eBay company, also known as “eBay Store”, accounts registered to the **SUBJECT PERSON**, that, as of the day of the application for this warrant, have retail products listed for sale, namely carolina\_otc (seller ID name is listed as Carolina\_OTC), emily-tastic (seller ID name is listed as emilys\_finds247), and olivertwistnc (seller ID name is listed as OLIVERTWIST’S SUPPLEMENTS AND MORE) (SUBJECT BUSINESSES), including any and all business, financial, and other financial records, to include but not limited to financial institution account records including statements, loan files, correspondence, check registers, canceled checks, deposit slips, ATM receipts, cashier’s checks, money orders, domestic and international wire transfers in and out of the accounts, and other methods of payment and other financial instrument, credit card bills, and other financial records;
- h. All records relating to the violations referenced above for the **SUBJECT PERSON** and SUBJECT BUSINESSES, including lists of customers and related identifying

information; types, amounts, and prices of retail merchandise sold, as well as dates, places, and amounts of specific transactions;

- i. Any and all records and information relating to eBay, and any other online marketplaces or forums through which **SUBJECT PERSON** and **SUBJECT BUSINESSES**, sold **STOLEN PRODUCT** online;
- j. Any and all records and information relating to the PayPal Account linked to or associated with the **SUBJECT PERSON** and **SUBJECT BUSINESSES**;
- k. Any and all records and information relating to the interstate shipment of parcels via United States Postal Service, UPS, FedEx, DHL, or any other commercial shipping carrier, including shipping labels, bills of lading, delivery service parcels, and any items related to the shipment of goods linked to the scheme;
- l. Any and all business records relating to the **SUBJECT PERSON** and **SUBJECT BUSINESSES**, including, but not limited to appointment books, calendars, and/or work schedules, receipt books, ledgers, journals, balance sheets, statements, summaries, schedules or other documentation pertaining to revenue, income, and compensation;
- m. All documents referencing storage facilities, safe deposit boxes, and/or rented post office boxes, other mailboxes and keys/passwords related to the same, including records relating to the rental, lease, or purchase of storage units, lockers, or safe deposit boxes, including contracts, payment receipts, keys, access records, and entry access codes;

- n. Any United States and foreign currency and other monetary instruments derived from fraud or the proceeds of fraud or otherwise whose origins cannot be determined;
- o. Any documents, records, programs or applications that identify the Internet service provided to the **SUBJECT PREMISES**;
- p. Records and information relating to the identity or location of the co-conspirators;
- q. Any records and information relating to any discussions of a plan or scheme to steal merchandise from commercial retailers, national drugstore chains, and national supermarket chains, such as CVS, Walgreens, Kroger, Target, Publix, Harris Teeter, Walmart, etc, and resell that stolen product online or through any other channel;
- r. Records, information, and items relating to the occupancy or ownership of the **SUBJECT PREMISES**, 422 Foster Lane, Pittsboro, NC, including utility and telephone bills, mail envelopes, or addressed correspondence, letters, receipts for rent or moneys paid, photographs, and personalized items;
- s. Records and recordings from video surveillance systems on the **SUBJECT PREMISES** that will aid investigators in identifying local boosters, delivery shipments, and employees reporting for work.
- t. Any laptop computers, desk top computers, electronic tablets, smart mobile telephones, and any other devices capable of storing data and accessing websites used as a means to commit the **SUBJECT OFFENSES** (“COMPUTERS”).
- u. During the course of the search, photographs of the searched premises may be taken to record the condition thereof and/or the location of items therein.



For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. Evidence of the lack of such malicious software;
- d. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- e. Evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;
- f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. Evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. Evidence of the times the COMPUTER was used;

- i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. Records of or information about Internet Protocol addresses used by the COMPUTER;
- l. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and routers, modems, and network equipment used to connect computers to the Internet.
- m. Records, information, and items relating to violations of the statutes described above;
- n. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
- o. Records and information relating to the identity or location of the persons suspected of violating the statutes described above.

As used above, the terms "records" and "information" includes all forms of creation or storage, specifically: any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); any photographic form (such as microfilm, microfiche, prints, slides, negatives,

videotapes, motion pictures, or photocopies); and any cloud storage (which the aforementioned electronic devices are connected to).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the **SUBJECT PREMISES** described in Attachment A, law enforcement personnel are also specifically authorized to compel Robert (“Bob”) OLIVER, if present at the time of the execution of the warrant, to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

- a. any of the devices found at the **SUBJECT PREMISES**, and
  - b. where the devices are limited to which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,
- for the purpose of attempting to unlock the devices’ security features in order to search the contents as authorized by this warrant, but only if Robert (“Bob”) OLIVER is present at the time of the



execution and the process is carried out with dispatch in the immediate vicinity of the **SUBJECT PREMISES**.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the **SUBJECT PREMISES** to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any device. Further, this warrant does not authorize law enforcement personnel to request that any individuals present at the **SUBJECT PREMISES** state or otherwise provide the password or any other means that may be used to unlock or access the devices, including by identifying the specific biometric characteristics (including unique finger(s)) or other physical features) that may be used to unlock or access the devices.